

# Instructions to Restrict a Microsoft XP Professional Machine on Active Directory to only to Select IDs at Lehigh University

David Morrisette

April 25, 2007

## Abstract

This is a set of instructions which illustrates how to set up a Microsoft Windows XP Professional machine at Lehigh University to use a restricted set of User IDs. The approach that is shown in the following pages is useful when you have a user, or set of users, that do not want other users to be able to log into their machines. These notes specifically pertain to a machine which is integrated with Lehigh University's Active Directory Domain. If steps are not taken, such as the steps in this documentation, then other individuals who have Lehigh University Active Directory IDs, other than the primary user(s) of the machine, have the ability to log onto the machine.

Note that this information can only be used by IT staff, or others, that have been given the appropriate permissions to administer Lehigh University Active Directory IDs. An ID and password is required to add and/or delete Active Directory ID within local groups on individual machines.

**Please proceed very carefully with these directions! If not done correctly, it is possible to entirely lock out access to a system for all users. Proceed carefully and with caution!**

## Contents

<b>1</b>	<b>Who is included in the Administrator Group</b>	<b>2</b>
<b>2</b>	<b>The Group Policy Editor Interface</b>	<b>3</b>
<b>3</b>	<b>Drill Down to Allow Log On Locally</b>	<b>4</b>
<b>4</b>	<b>Group Policy Restrictions on Who Can Log in Locally</b>	<b>5</b>
<b>5</b>	<b>Remove <i>AD\Domain Users</i> from the Users Group</b>	<b>6</b>

# 1 Who is included in the Administrator Group



Figure 1: Who is in the Administrator Group

The first thing we will look at is a typical setup of a faculty members machine. In Figure 1, we can see from looking at the local machine's Administrators group Properties that there are several objects assigned to the local machine's Administrators group. The objects assigned to the Administrators group are as follows:

**AD\DomainAdmins** Domain Administrators

**AD\eng-workgrp-mgr** Engineering Work Group Manager

**AD\tjl3** AD User ID

**Administrator** Local Administrator ID

**plg** Local "backdoor" password protected userid for EECS administrators' use

The screen seen in Figure 1 is the "normal" place we set up our groups when following our standard directions for setting up a machine on Active Directory. This screen can be displayed by clicking on *start* ⇒ *Control Panel* ⇒ *Administrative Tools* ⇒ *Computer Management* ⇒ *Local Users and Groups* ⇒ *Groups* ⇒ right click Groups and select Properties.

## 2 The Group Policy Editor Interface

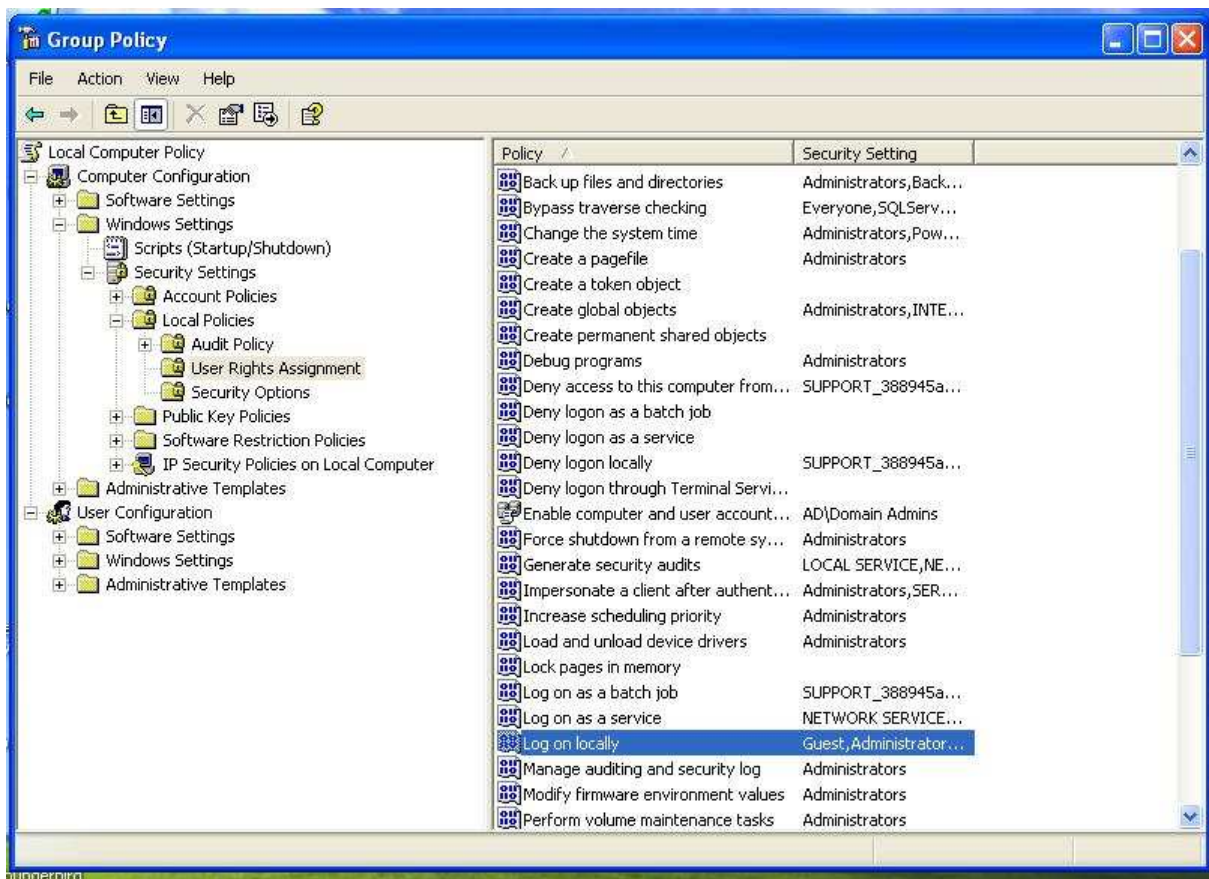


Figure 2: The Group Policy Editory Interface

The next three pages are not necessary for the actual process of restricting a computer to specific user IDs, but are just being shown to help explain why what we are doing works. If you should set up a computer to restrict access of unwanted users (in our case *Domain Users*), I would suggest that you do not run the screens in Figure 2 and Figure 3.

We are going to look at the *Group Policy Editor*, which is a program that has read and write access to the *registry*. Within the *Group Policy Editor* is a section that indicates what groups and users can log in locally to a local machine.

In order to start the *Group Policy Editor*, you can type the command *gpedit.msc* at the command prompt. After entering the command *gpedit.msc* at the command line, you should see the interface of the Group Policy Editor, similar to what is shown in Figure 2. Using this tool, there are many things that can be changed regarding the way the system behaves. We will only be addressing restricting access to individuals that would sit down and try to log into a machine from the keyboard.

### 3 Drill Down to Allow Log On Locally



Figure 3: Drill down to *Allow Log On Locally* Policy

In order to navigate to the *Policy* that we want to examine, the path to click on will be as listed below:

- Computer Configurations
- Windows Settings
- Security Settings
- Local Policies
- User Rights Assignment
- Allow log on locally

Notice the five groups that by default are allowed to log in locally on XP Professional. As you can see in Figure 3 are the groups of Administrator, Backup Operators, Guest, Power Users, and User. In order to keep Active Directory users that are not administrators from accessing this machine, we need to examine other types of Active Directory objects (user ids or groups) that might be in one of the above listed groups that have the ability to log on locally.

## 4 Group Policy Restrictions on Who Can Log in Locally

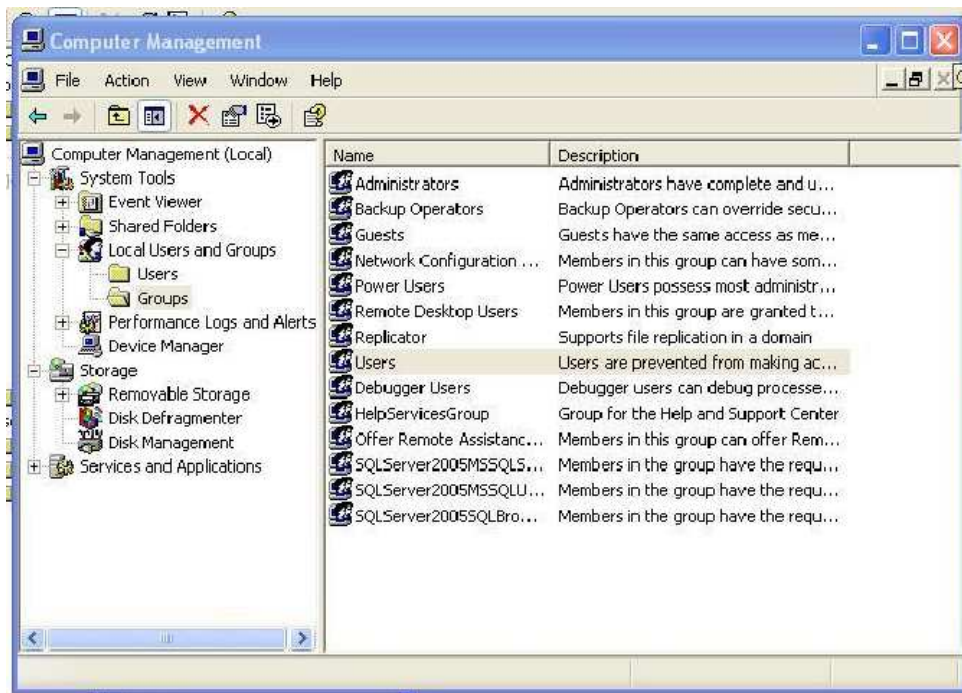


Figure 4: The Users group needs modification

After examining the five groups listed in Figure 3, and seeing what objects are within those groups, we will find that the Users group is the likely candidate for modification. The *Users* group has the object *Domain Users* listed within it.

Highlight the *Users*, do a right click and select Properties. You should then see a screen similar to what you will see on 5 on the following page.

## 5 Remove *AD\Domain Users* from the Users Group

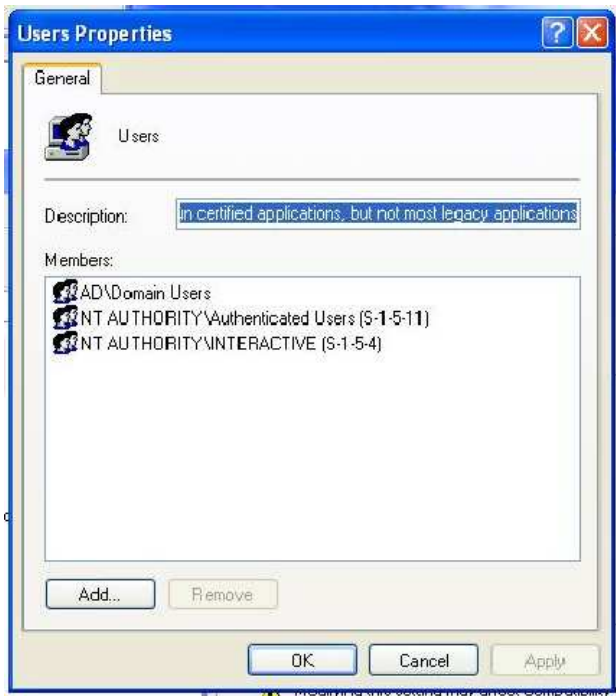


Figure 5: Remove *AD\Domain Users*

If you remove the Active Directory Group *AD\Domain Users* from the *Users* Group Properties, then non-administrative Active Directory accounts will not be able to log into the machine from the keyboard.